Schrems II – A brief history, an analysis and the way forward

Shreya Tewari 2020-07-25T16:00:00

On July 16, 2020, the European Court of Justice (ECJ) invalidated the EU-US Privacy Shield – a framework that regulated Trans-Atlantic data transfers. Further, even though the court upheld the validity of Standard Contractual Clauses (SCC) – an EU-approved template to safeguard EU citizens' data-transfer, it put forth important qualifications for data controllers to adhere to when using such SCCs.

This article analyses the ECJ's ruling, now known as *Schrems II*, in three parts. The *first* section sets the stage for the analysis by providing a brief history of EU-US data-flow arrangements and the developments leading up to *Schrems II*. The *second* section analyses the ECJ's decision in *Schrems II* and finally, the *third* section concludes by exploring the implications of the ruling and evaluating the way forward.

Introduction and brief history

The European Union's (EU) Charter of Fundamental Rights grants every EU citizen the right to have their data processed fairly, for specified purposes, and with user consent. The General Data Protection Regulation (GDPR) expounds on this right by providing adequate safeguards protect personal data that belongs to EU citizens. It further clarifies that data-transfers to third countries are conditional upon an adequate level of data protection in those third countries.

Until 2015, the Safe Harbour Agreement was an EU-US data flow arrangement between the US Department of Commerce and the European Union that regulated cross-Atlantic data transfer and was said to meet the abovementioned level of 'adequate protection'. In 2013, Max Schrems, an Austrian privacy rights campaigner, challenged the validity of this agreement and specifically, the transfer of his personal data (and EU members' personal data) by Facebook to servers based in the United States of America (US), before the Irish Data Protection Commission. Once his initial complaint was rejected, he moved to the country's High Court. The High Court, in turn, referred the case to the ECJ. After considering the safe harbour principles' adequacy to protect EU citizen's data and in light of the Snowden surveillance revelations, the ECJ found them to be invalid in 2015 (in a ruling famously known as *Schrems I*).

Within a few months, the European Commission and the USA's Department of Commerce, once again, came together to draft an alternative framework that provided an adequate level of data protection to trans-Atlantic data transfers. Resultantly, the safe harbour agreement was replaced by the EU-US Privacy Shield. The EU-US Privacy Shield was designed to ensure consistency with EU Laws when

transferring data of EU citizens into the US. Alternatively, controllers could adhere to Standard Contractual Clauses that were pre-approved by the European Commission and would act as the terms and conditions for extraterritorial data-transfers. It is important to note here that SCCs had been recognised by the Commission in 2010 itself. The EU-US Privacy Shield, in particular, was heavily criticised by activists and data protection experts alike for not providing any concrete protection against indiscriminate access to personal data for national security purposes.

The Schrems II case

In 2015, Schrems once again challenged Facebook's use of SCCs to transfer EU citizens' data to the USA on the ground that it did not adequately protect the rights of the EU-based data subjects. The Irish Data Protection Commission referred the case to the Irish High Court and the High Court, in turn, referred the case to the ECJ in 2018 for a preliminary ruling. This article will focus on the two main questions raised by the High Court that broadly cover the thematic issues raised in the other questions – these include *first*, the validity of the EU-US Privacy Shield and *second*, the validity of SCCs.

With regard to the *first question*, the ECJ found the EU-US Privacy Shield to be invalid. At the outset, the ECJ noted that to find the EU-US Privacy Shield to be adequate, it had to be satisfied that the domestic law of the third country guaranteed a level of protection of fundamental rights 'essentially equivalent' to that which was guaranteed under EU Law (Para 162). Consequently, the Court found it necessary to assess whether certain provisions of the US's Foreign Intelligence Surveillance Act and the subsequent surveillance programmes that such provisions empower, ensures an adequate level of protection subject to, of course, the test of proportionality.

The ECJ found that the limitations on the protection of personal data that arose from US laws did not satisfy the 'essential equivalence' requirement. It found that the surveillance programmes based on such legal provisions are not proportional and 'strictly necessary' (Para 184). The Court noted that US's primacy to national security, public interest and law enforcement allowed for interference with the fundamental rights of persons whose data is transferred to the US. For instance, it observed that the US Government did not grant data subjects actionable rights before the US Courts against US authorities. Further, it held that the mechanisms incorporated in the EU-US Privacy shield that were intended to mitigate these harms did not meet the required legal standard of 'essential equivalence' with EU Law. On these grounds, the ECJ found the EU-US Privacy Shield to be inadequate and invalid.

Regarding the *second question*, the ECJ found the Standard Contractual Clauses to be valid – albeit with qualifications to ensure adequate data protection. It noted that in cases where SCCs were the basis of data transfer in a third country, the level of protection of an EU citizen's data in that third country must be 'essentially equivalent' to the level of protection that has been guaranteed under the GDPR.

The ECJ went on to clarify that a third country's level of protection had to be assessed by taking into consideration the SCCs themselves and also the relevant legal system of the jurisdiction to which the data would be transferred. The latter consideration intends to ensure that the standard of 'essential equivalence' is met. For determining essential equivalence, the appropriate safeguards, enforceable rights and effective legal remedies of the third country must be taken into consideration (Para 104 and 105). The ruling on this matter was in line with the ECJ's Advocate General's opinion issued in December 2019.

Implications and the way forward

With this ruling, the ECJ has reiterated its strong commitment to upholding EU citizens' fundamental right to have their data processed fairly, with consent and for specified purposes. Not only has the Court invalidated the EU-US Privacy Shield, but it has also required all member states' Data Protection Authorities to suspend transfers of data through SCCs to third countries where the level of data protection maintained in the EU cannot be met.

The Court has categorically clarified that since the domestic laws and surveillance programmes in the US do not meet the test of proportionality, its data protection framework is not 'essentially equivalent' to the EU's.

In the aftermath of the *Schrems II* ruling, V#ra Jourova, the Vice President of the European Commission for Value and Transparency has stated in an official press conference that the European Commission will work with their American counterparts to discuss a way forward. It is possible that they will reformulate an alternate mechanism that accommodates data transfer between the EU and USA.

However, a strict reading of the ECJ's ruling calls for the US to review its surveillance laws before the EU can resume data-transfer with US-based organisations. In this regard, nyob, an organisation founded by Schrems, noted in its first statement after the ruling that the US would have to "engage in serious surveillance reform to get back to a 'privileged' status for US companies". We live in a post-Snowden era and are cognisant that Facebook, Apple, Microsoft, and Google were some of the many companies feeding data to the National Security Agency for a mass surveillance programme and this exchange of data was permitted by provisions under The Foreign Intelligence Surveillance Act (FISA). Through this landmark judgment, the ECJ has not only made a stronger case for data protection, but it has also, in some ways, pushed for a surveillance reform and an adequate data protection framework for countries that hope to serve a customer base in the EU. This judgement is a concrete step in the right direction for many reasons, including the fact that it pushes for surveillance reforms. It is also a cautionary tale for developing economies such as India, where the data protection framework is at the cusp of taking shape.

The ECJ also clarifies the role of Data Protection Commissions in determining the adequacy of SCCs. Even though the GDPR does not explicitly require them to do so, the ruling authorises the Data Protection Commissions to examine the adequacy

standards of SCCs based on complaints received by individuals and to restrict or prohibit the transfer of data if the data protection standards are inadequate. This will ensure better enforceability of the judgment since the ECJ has decentralised the authority for making adequacy decision to the various Data Protection Commissions in the EU states. Even so, the European Commission will continue to have the final say. Its adequacy decisions will remain binding.

Lastly, the ruling has also led various US-based organisations to immediately switch from the EU-US Privacy Shield framework to SCCs. Having said that, as mentioned earlier, the standard of due diligence that such organisations would have to engage in has increased considerably. As the ruling mentioned, not only should the organisation internally comply with the SCCs, it must also ensure that the jurisdiction in which the data is held is essentially equivalent to the standards of data protection in the EU. Hence, while the decision regarding the EU-US Privacy Shield is a clean-cut in that it provides absolute clarity, the decision regarding the SCCs is nebulous. As Daniel J Solove notes, the ECJ has put SCCs in a coma on life support. This is because the ECJ found that the SCCs could not be used for data transfer to US without additional protection against US surveillance. It is also a possibility that due to this, the organisations with servers in the US would try to switch to data processing within Europe and silo data within the EU.

In any case, the *Schrems II* judgment is a landmark decision which sets a valuable precedent for extraterritorial data-transfers and raises some interesting questions that will have to be addressed in through partnerships between legislators, data protection experts, tech industrialists and activists alike.

(cc) BY-NC-ND